

Personal information. Information about an individual that identifies, relates or is unique to, or describes him or her; e.g., a social security number, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, etc.

Privacy Act request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

Member of the public. Any individual or party acting in a private capacity to include federal employees or military personnel.

Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc.), about an individual that is maintained by a DoD Component, including but not limited to, his or her education, financial transactions, medical history, criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Risk assessment. An analysis considering information sensitivity, vulnerabilities, and the cost to a computer facility or word processing activity in safeguarding personal information processed or stored in the facility or activity.

Routine use. The disclosure of a record outside the Department of Defense for a use that is compatible with the purpose for which the information was collected and maintained by the Department of Defense. The routine use must be included in the published system notice for the system of records involved.

Statistical record. A record maintained only for statistical research or reporting purposes and not used in whole or in part in making determinations about specific individuals.

System manager. The DoD Component official who is responsible for the operation and management of a system of records.

System of records. A group of records under the control of a DoD Component from which personal information is retrieved by the individual's name or by

some identifying number, symbol, or other identifying particular assigned to an individual.

Word processing system. A combination of equipment employing automated technology, systematic procedures, and trained personnel for the primary purpose of manipulating human thoughts and verbal or written or graphic presentations intended to communicate verbally or visually with another individual.

Word processing equipment. Any combination of electronic hardware and computer software integrated in a variety of forms (firmware, programmable software, handwiring, or similar equipment) that permits the processing of textual data. Generally, the equipment contains a device to receive information, a computer-like processor with various capabilities to manipulate the information, a storage medium, and an output device

§ 318.4 Policy.

(a) It is DTRA policy that:

(1) The personal privacy of an individual shall be respected and protected. Personal information shall be collected, maintained, used, or disclosed to insure that:

(2) It shall be relevant and necessary to accomplish a lawful DTRA purpose required to be accomplished by Federal statute or Executive order;

(3) It shall be collected to the greatest extent practicable directly from the individual;

(4) The individual shall be informed as to why the information is being collected, the authority for collection, what uses will be made of it, whether disclosure is mandatory or voluntary, and the consequences of not providing the information;

(5) It shall be relevant, timely, complete and accurate for its intended use; and

(6) Appropriate administrative, technical, and physical safeguards shall be established, based on the media (e.g., paper, electronic, etc.) involved, to ensure the security of the records and to prevent compromise or misuse during storage or transfer.

(b) No record shall be maintained on how an individual exercises rights guaranteed by the First Amendment to

the Constitution, except as specifically authorized by statute; expressly authorized by the individual on whom the record is maintained; or when the record is pertinent to and within the scope of an authorized law enforcement activity.

(c) Notices shall be published in the FEDERAL REGISTER and reports shall be submitted to Congress and the Office of Management and Budget, in accordance with, and as required by 5 U.S.C. 552a, OMB Circular A-130, and 32 CFR part 310, as to the existence and character of any system of records being established or revised by the DoD Components. Information shall not be collected, maintained, or disseminated until the required publication/review requirements are satisfied.

(d) Individuals shall be permitted, to the extent authorized by this part:

(1) To determine what records pertaining to them are contained in a system of records;

(2) Gain access to such records and obtain a copy of those records or a part thereof;

(3) Correct or amend such records on a showing the records are not accurate, relevant, timely, or complete.

(4) Appeal a denial of access or a request for amendment.

(e) Disclosure of records pertaining to an individual from a system of records shall be prohibited except with the consent of the individual or as otherwise authorized by 5 U.S.C. 552a and 32 CFR part 286. When disclosures are made, the individual shall be permitted, to the extent authorized by 5 U.S.C. 552a and 32 CFR part 310, to seek an accounting of such disclosures from DTRA.

(f) Computer matching programs between DTRA and Federal, State, or local governmental agencies shall be conducted in accordance with the requirements of 5 U.S.C. 552a, OMB Circular A-130, and 32 CFR part 310.

(g) DTRA personnel and Systems Managers shall conduct themselves, pursuant to established rules of conduct, so that personal information to be stored in a system of records shall only be collected, maintained, used, and disseminated as authorized by this part.

§ 318.5 Designations and responsibilities

(a) The Director, DTRA shall:

(1) Provide adequate funding and personnel to establish and support an effective Privacy Program.

(2) Appoint a senior official to serve as the Agency Privacy Act Officer.

(3) Serve as the Agency Appellate Authority.

(b) The Privacy Act Officer shall:

(1) Implement the Agency's Privacy Program in accordance with the specific requirements set forth in this part, 5 U.S.C. 552a, OMB Circular A-130, and 32 CFR part 310.

(2) Establish procedures, as well as rules of conduct, necessary to implement this part so as to ensure compliance with the requirements of 5 U.S.C. 552a, OMB Circular A-130, and 32 CFR part 310.

(3) Ensure that the DTRA Privacy Program periodically shall be reviewed by the DTRA Inspectors General or other officials, who shall have specialized knowledge of the DoD Privacy Program.

(4) Serve as the Agency Initial Denial Authority.

(c) *The Privacy Act Program Manager shall:*

(1) Manage activities in support of the DTRA Program oversight in accordance with part, 5 U.S.C. 552a, OMB Circular A-130, and 32 CFR part 310.

(2) Provide operational support, guidance and assistance to Systems Managers for responding to requests for access/amendment of records.

(3) Direct the day-by-day activities of the DTRA Privacy Program.

(4) Provide guidance and assistance to DTRA elements in their implementation and execution of the DTRA Privacy Program.

(5) Prepare and submit proposed new, altered, and amended systems of records, to include submission of required notices for publication in the Federal Register consistent with this part, 5 U.S.C. 552a, OMB Circular A-130, and 32 CFR part 310.

(6) Prepare and submit proposed DTRA privacy rulemaking, to include documentation for submission of the proposed rule to the Office of the Federal Register for publication. Additionally, provide required documentation